IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF 3009 SUMMERSHADE COURT HERNDON, VIRGINIA 20171	**UNDER SEAL** 1:22-SW-372

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A SEARCH AND SEIZURE WARRANT

I, Randall M. Mason, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 3009 Summershade Court, Herndon, Virginia 20171 ("**TARGET LOCATION**") further described in Attachment A, for the things described in Attachment B.

2. As explained herein, based on my training and experience, and the facts set forth in this affidavit, I submit there is probable cause to believe that ISAIAS DANIEL CHINCHILLA (hereinafter, "CHINCHILLA") is involved in a conspiracy to distribute fentanyl, in violation of Title 21, United States Code, Sections 841(a)(1) and 846. There is also probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as further described in Attachment B, will be found at the **TARGET LOCATION.**

3. I am a Detective with the Arlington County Police Department. I have been employed as a police officer with the Arlington County Police Department since 2007. I have been assigned to the Vice/Narcotics Unit since 2014. I am currently assigned to the Drug Enforcement Administration ("DEA"), where I am federally deputized as a Task Force Officer ("TFO") with the DEA's High Intensity Drug Trafficking Area Task Force. As such, I am a Law

Enforcement Officer as defined under Section 2510(7) of Title 18, United States Code, (*i.e.* an officer of the United States or a political sub-division thereof, who is empowered to conduct investigations of, and to make arrests for, offenses enumerated in Title 21, United States Code). During my time in law enforcement, I have participated in the application for and execution of numerous arrest and search warrants in the investigation of narcotics and organized crime related offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, weapons, stolen property, and other evidence of criminal activity.

4. During my time in law enforcement, I have investigated violations of federal and state narcotics laws. I have conducted or participated in numerous investigations involving narcotics-related offenses, which have resulted in the seizure of illegal drugs, drug proceeds in the form of United States currency, weapons, and other evidence of criminal activity. My experience includes the execution of search warrants. These investigations have led to the arrest and conviction of drug distributors and users in the General District, Juvenile and Domestic Relations, and Circuit Courts of Arlington County, as well as in the Eastern District of Virginia. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology used by drug traffickers and abusers of controlled dangerous substances. Through my employment, I have gained knowledge in the use of various investigative techniques including the use of wiretaps, physical surveillance, undercover agents, confidential informants and cooperating witnesses, the controlled purchase of illegal narcotics, electronic surveillance, consensually monitored recordings, investigative interviews, financial investigations, the service of administrative and grand jury subpoenas, and the execution of search and arrest warrants. I have testified at trials, in grand jury proceedings, and at preliminary hearings, and I have been

certified as an expert in the distribution of narcotics in Arlington County General District and Circuit Courts.

5. The facts and information contained in this affidavit are based upon my personal knowledge of the investigation and observations of other law enforcement officers and agents involved in this investigation. All observations referenced below that were not personally made by me were relayed to me by the persons who made such observations. Additionally, unless otherwise noted, wherever your Affiant asserts that a statement was made by an individual, such statement is described in substance herein, and is not intended to be a verbatim recitation of such statement.

6. This affidavit contains information necessary to support probable cause. The information contained in this affidavit is not intended to include each and every fact and matter observed by or known to the United States.

7. Based on my training and experience, I am aware that:

a. Individuals who distribute illegal controlled substances often maintain records relative to their drug trafficking activities. These records and documents are usually secreted in their places of residence, or the residences of family members, friends, or associates, in their businesses, or in the places of operation of the drug distribution activity such as a stash house or safe house. These documents often include ledgers, account books, calculations, or other notations which reflect inventories and quantities of narcotics purchased and distributed. The documents also may include "pay-owe sheets," which are documents that bear calculations, customers' names, quantities, and prices.

b. Individuals who distribute illegal controlled substances maintain documents, letters, and records relating to the illegal activity for periods of time. This

documentary evidence is usually secreted in their places of residence, or the residences of family members, friends, or associates, in their businesses, or in the places of operation of the drug distribution activity such as a stash house or safe house. This documentary evidence includes, but is not limited to, telephone numbers, telephone books, address books, credit card receipts, hotel receipts, train and bus tickets, car rental receipts, amounts and records in fictitious names, false identification documents, money orders, account notations, "pay-owe sheets," and other records indicating the existence of storage facilities used in narcotics trafficking. In my training and experience, I also know that individuals who have committed crimes using computers often keep records of their crimes in digital or electronic format, such as on a computer, and that computers are often stored in a residence.

c. Individuals who distribute illegal controlled substances commonly maintain addresses or telephone numbers in books or papers, which reflect names, addresses and/or telephone numbers of their associates in drug trafficking. They also store such information, as well as photographs, messages, and personal notes, in electronic equipment including, but not limited to, computers, cellular phones, and other electronic software and mediums.

d. Individuals who distribute illegal controlled substances often maintain, on hand and in their residences, large amounts of U.S. currency in order to maintain and finance their ongoing criminal activities.

e. Individuals who distribute illegal controlled substances often use, carry, and retain firearms and other weapons to protect themselves, as well as to secure their cache of narcotics and the proceeds of their drug trafficking. Individuals who possess and

store firearms in their residences, vehicles and/or stash locations, or in the residences of trusted associates, often also store ammunition, shell casings, slugs, targets, holsters, gun cleaning kits, and ownership papers in those locations.

f. Individuals who distribute illegal controlled substances commonly maintain currency, controlled substances, firearms, and other contraband in locked containers such as a safe.

g. Individuals who distribute illegal controlled substances take, or cause to be taken, photographs of themselves and their associates in the drug trade, property derived from the distribution of narcotics, and their products, and such photographs are often kept in their residence. Individuals who distribute illegal controlled substances commonly keep packaging materials, scales, and other drug paraphernalia in their residences and on their property.

PROBABLE CAUSE

8. The United States, including the DEA, is conducting a criminal investigation of CHINCHILLA and others regarding possible violations of 21 U.S.C. §§ 841(a)(1) and 846 (Conspiracy to Distribute Fentanyl).

9. During the month of February 2022, Loudoun County Sheriff's Office ("LCSO") Detective James Lim received information from a confidential cooperating source ("CS-1") that an unindicted co-conspirator ("UCC-1") was distributing Percocet pills in Loudoun County, which is within the Eastern District of Virginia. For the purposes of this Affidavit, the cooperating source will be referred to in the masculine gender, regardless of whether the CS is in fact male or female.

10. CS-1 became a source of information with LCSO in or about February 2022 following his arrest for distribution of a controlled substance. CS-1 is an admitted drug user and distributor. Apart from the February 2022 arrest, CS-1 has no additional criminal history. The information that CS-1 has provided to law enforcement has been proven true and accurate. With respect to the instant case, CS-1's information has been corroborated by other confidential sources, information obtained from various public databases, physical surveillance, and other information obtained during the investigation. To my knowledge, none of the information provided by CS-1 has proved to be false, misleading, or inaccurate in any material respect. CS-1 has made statements against his own penal interest. For these reasons, I consider CS-1 to be reliable.

11. During the months of February and March, CS-1 conducted four controlled purchases in the Eastern District of Virginia for a total of approximately 370 pills. During the first controlled purchase, UCC-1 gave CS-1 the Snapchat account name "ZBANDZ_23" to contact for future purchases. UCC-1 identified the user of the account as UCC-1's source of supply.

12. CS-1 utilized the "ZBANDZ_23" Snapchat account to arrange the second, third, and fourth controlled purchases that CS-1 performed. CHINCHILLA was present for all three of those purchases and UCC-1 was involved with the first, second, and fourth controlled purchases. An undercover detective ("UC-1") accompanied CS-1 to some of these purchases and was ultimately introduced to CHINCHILLA. Following the fourth controlled purchase, surveillance followed the vehicle CHINCHILLA was in to the neighborhood of the TARGET LOCATION but not to the TARGET LOCATION specifically.

13. Between late March and mid-May 2022, UC-1 conducted four controlled purchases from CHINCHILLA by contacting him on Snapchat. In each of these four controlled purchases, UC-1 contacted the "ZBANDZ" Snapchat account and CHINCHILLA was the individual who came to perform the deal. In each of these deals, CHINCHILLA met UC-1 at a predetermined location within the Eastern District of Virginia. In each deal, CHINCHILLA got into UC-1's vehicle and UC-1 handed CHINCHILLA pre-recorded law enforcement buy funds ("buy funds"). During the first two deals, CHINCHILLA directed UC-1 to a nearby car where the pills were located on a parked car's tire. In the third and fourth deal, UC-1 handed buy funds directly to CHINCHILLA and CHINCHILLA handed a quantity of pills directly to UC-1. Prior to the third and fourth controlled purchases, which occurred on April 27, 2022 and May 12, 2022 respectively, law enforcement set up surveillance on the TARGET LOCATION prior to the deal. Surveillance observed CHINCHILLA exit the TARGET LOCATION, enter a vehicle, and maintained surveillance to the deal location.

14. Over the course of the five aforementioned controlled purchases, UC-1 purchased approximately 529 pills believed to contain fentanyl for $6990. Those 529 pills were similar in size, shape, and markings to the 370 pills previously purchased by CS-1. Additionally, CHINCHILLA admitted to UC-1 during one of the deals that CHINCHILLA knew the pills contained fentanyl. Each of the four quantities of pills were sent to the Virginia Department of Forensic Sciences for analysis. Two of the quantities have been tested and came back as containing fentanyl, a Schedule II substance. The results on the final two quantities are still pending.

15. On or about June 10, 2022, UC-1 contacted CHINCHILLA through Snapchat and arranged to purchase 100 pills believed to contain fentanyl for $1300. Law enforcement set up

surveillance on the TARGET LOCATION and observed CHINCHILLA exit the TARGET LOCATION and get into a passenger seat of a waiting car. Surveillance followed CHINCHILLA to a location within the Eastern District of Virginia where CHINCHILLA and UC-1 met. UC-1 received 100 pills in exchange for $1300. UC-1 handed buy funds directly to CHINCHILLA who handed UC-1 the bag containing 100 pills. Following the deal, Detective Lim counted the pills and confirmed that UC-1 had received 100 pills. The pills were similar in size, shape, and marking to the previous pills purchased from CHINCHILLA. Those pills have been sent to the Virginia Department of Forensic Science for analysis and results are pending.

16. On or about June 23, 2022, UC-1 contacted CHINCHILLA through Snapchat and arranged to purchase 250 pills believed to contain fentanyl for $2500. Law enforcement set up surveillance on the TARGET LOCATION and observed CHINCHILLA exit the TARGET LOCATION and get into a passenger seat of a waiting car. Surveillance followed CHINCHILLA to a location within the Eastern District of Virginia where CHINCHILLA and UC-1 met. UC-1 received 250 pills in exchange for $2500. UC-1 gave buy funds directly to CHINCHILLA who handed UC-1 a bag containing 250 pills. UC-1 inquired about making a larger purchase, such as 400-500 pills, from CHINCHILLA on the next deal. CHINCHILLA stated that he would have no problem fulfilling that order and stated that he currently had access to 10,000 pills. Following the deal, Detective Lim counted the pills and confirmed that UC-1 had only received 249 pills. The pills were similar in size, shape, and marking to the previous pills purchased from CHINCHILLA. Those pills have been sent to the Virginia Department of Forensic Science for analysis and results are pending.

17. CHINCHILLA is being supervised in relation to separate charges in Fairfax County. In connection with that supervision, CHINCHILLA provided the TARGET LOCATION as his current residence.

18. As part of the investigation in this case, Your Affiant ran record checks through the Virginia Department of Motor Vehicle's database. Through those checks, Your Affiant learned that CHINCHILLA has a valid Virginia learner's permit. The TARGET LOCATION is listed as CHINCHILLA's address on the permit. These records also reflect that CHINCHILLA's Virginia learner's permit transcript has a prior address listed on it, but the current address listed on the transcript is the TARGET LOCATION. The address change was made on January 31, 2022.

USE OF CELLULAR TELEPHONES/STORAGE MEDIA BY DRUG TRAFFICKERS

19. Based on my training, experience, and participation in narcotics and drug-related investigations, and my knowledge of this case, I am aware that:

a. Drug traffickers commonly utilize cellular phones, as well as other communication devices, to keep in constant contact with their suppliers, associates, and clients in drug trafficking.

b. Drug traffickers commonly utilize and possess multiple cellular phones at any given time. It is common for drug traffickers to use one cell phone as a personal number that they attempt to limit the numbers of contacts with other co-conspirators involved in their trade. Drug traffickers commonly utilize a second phone as their "work" phone that is used in their business. This second phone utilized for business purposes is often not in the drug trafficker's name. The second phone is also commonly changed, either by changing phones entirely or changing the phone number of the second phone.

All of these things are done by drug traffickers in an attempt to avoid detection by law enforcement.

c. Drug traffickers commonly make and maintain business records. Specifically, it is quite common for those involved in the manufacture, sale, purchase, and transportation of controlled substances to generate and maintain writings, books, records, receipts, notes, ledgers, lists, airline tickets, money orders, package and shipping labels, and other memoranda to assist in their criminal activities. These materials are created and maintained in much the same way and for the same reasons as persons involved in legitimate businesses. Drug traffickers maintain records in order to know the current status of the various illegal transactions in which they are involved. Without the aid of such records, drug traffickers would face a high possibility of error and mistake due to the number, complexity, and frequency of their transactions, and the clandestine nature of drug trafficking activities. These business records are often located within the contents of the drug trafficker's cell phone(s).

d. Drug traffickers commonly maintain addresses or telephone numbers in books or papers, which reflect names, addresses and/or telephone numbers of their associates in drug trafficking. They also store such information, as well as photographs, messages, and personal notes, in electronic equipment including, but not limited to, cellular phones.

e. Drug traffickers commonly keep their old cell phones. It is common for law enforcement to seize numerous old cell phones during the execution of a search warrant at a drug trafficker's residence.

20. In my training and experience, it is likely that the **TARGET LOCATION** will contain at least one cellular phone because of the use of cellular phones in furtherance of the conspiracy to distribute controlled substances described above.

21. Further, I know that CHINCHILLA has used cellular phones to communicate through Snapchat about drug transactions with UC-1 and other individuals involved in drug distribution. As detailed herein, UC-1 has communicated with CHINCHILLA by cellular phone through Snapchat to coordinate drug transactions.

22. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing

the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search of the TARGET LOCATION. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel

may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the

device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the TARGET LOCATION and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled cellular phone device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock any cellular phone as described above within the attempts permitted by Touch ID or Face ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

23. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the TARGET LOCATION and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include cellular telephones, hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

25. As described above and in Attachment B, this application seeks permission to search for records that might be found at the property described in Attachment A, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including a cellular phone. Thus, the warrant

would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. *Probable cause*. I submit that if a computer or storage medium, including a cellular telephone, is found at the property described in Attachment A, there is probable cause to believe that it will include evidence, contraband, fruits, and/or instrumentalities of criminal activities for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and

virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate and search not only computer files that might serve as direct evidence of the crimes described on the warrant, but also seeks permission to locate and search forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the property described in Attachment A because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation

information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at the property described in Attachment A. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I am applying would permit seizing, imaging, or otherwise copying storage media that reasonably appears to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

< CONTINUED ON NEXT PAGE >

CONCLUSION

30. Based on the information provided in this affidavit, your Affiant submits that probable cause exists to believe that that ISAIAS DANIEL CHINCHILLA (hereinafter, "CHINCHILLA") is involved in a conspiracy to distribute fentanyl, in violation of Title 21, United States Code, Sections 841(a)(1) and 846. There is also probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as further described in Attachment B, will be found at the **TARGET LOCATION**. Wherefore, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I respectfully request warrants to search and authority to seize at the **TARGET LOCATION** those items identified in Attachment B.

Respectfully submitted,

Task Force Officer Randall M. Mason
Drug Enforcement Administration

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on July 6, 2022.

Digitally signed by Ivan Davis
Date: 2022.07.06 13:06:01 -04'00'

Hon. Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Place to be searched

The premises to be searched is the following, including any and all structures located within the curtilage thereof: 3009 Summershade Court, Herndon, Virginia 20171 **("TARGET LOCATION")** is a two-story single-family residence. The sides of the residence are a mixture of gray siding and red brick. The numbers "3009" are affixed horizontally above glass sliding doors on the left side of the residence and vertically on a post that supports the awning to the right of the main front door. The main door to the residence is white in color and is located in the middle of the residence.

ATTACHMENT B

Items to be seized

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841 and 846 (Conspiracy to distribute fentanyl) including, but not limited to, the following:

a. Controlled substances, indicia of distribution, records and documents, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of controlled substances;

b. Items commonly associated with the packaging and sales of controlled substances, including USPS packaging, sealed parcels prepared for mailing, gray and manila bubble mailers, address labels, black foil bags, plastic bags or zip lock bags;

c. U.S. currency and other illicit gains from the distribution of controlled substances;

d. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of controlled substances;

e. Address and/or telephone books and papers, including computerized or electronic addresses and/or telephone records reflecting names, addresses and/or telephone numbers;

f. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, controlled substances;

g. Firearms, ammunition (including spent ammunition), and indicia of firearm possession, including photos and videos depicting firearm possession, gun cases, gun packaging, gun racks, gun manuals, cleaning kits, tools used for the maintenance of firearms, magazines, ammunition, and packaging for magazines or ammunition;

h. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;

i. Cellular telephones, personal data accessories, computer flash cards, video tapes, compact disks, digital video disks, and other devices and/or electronic media;

j. Photographs and/or video, in particular photographs and/or videotapes of potential

co-conspirators and their criminal associates, assets, and/or controlled substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators;

k. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant ("COMPUTER"):

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. Evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. Evidence of the times the COMPUTER was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. Records of or information about Internet Protocol addresses used by the COMPUTER;

l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records," "documents," "programs," "applications," "materials," and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the **TARGET LOCATION** described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same

individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

This warrant authorizes the seizure of any COMPUTER or electronic device. However, with respect to any COMPUTER or electronic device, this warrant authorizes only the search of any COMPUTER or electronic device that is reasonably determined to have been owned or utilized by CHINCHILLA.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the DEA may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Any locked container such as a safe may be searched for the property to be seized set forth herein.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do *not* involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (*e.g.*, the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.